Dnro TRAFICOM/299376/03.03.01/2019
5.9.2019

Lausunto: KOMISSION SUOSITUS 5G-VERKKOJEN KYBERTURVALLISUUDESTA

1 5G tuo kuluttajien ja elinkeinoelämän saataville uusia palveluita

Matkapuhelinverkkojen kehitys alkoi NMT-teknologiasta, joka mahdollisti puhelut. 2G teknologian myötä puheluita alettiin siirtää digitaalisesti, mikä paransi tietoturvaa. 2G mahdollisti myös datayhteydet käyttäjille. 3G- ja 4G-teknologiat pääsääntöisesti paransivat tiedonsiirtokapasiteettia ja lyhensivät viiveitä. 3G ja 4G teknologiat ovat myös tuoneet turvallisuusominaisuuksia.

Kuten komission suosituksessa todetaan, 5G tuo mukanaan uusia palvelumahdollisuuksia loppukäyttäjille, mutta myös merkittäviä muutoksia verkkoarkkitehtuuriin. Uudet monimuotoisemmat palvelut tarkoittavat sitä, että 5G teknologian myötä matkapuhelinverkkojen merkitys jokapäiväisessä elämässä korostuu, esimerkiksi älyliikenteen myötä. Jotta yhteiskunta toimii sujuvasti, tulee palveluiden olla luotettavia. Jotta nämä monimuotoiset palvelut ovat mahdollisia, 5G määrittelee muutoksia operaattorien ylläpitämiin matkapuhelinverkkoihin. Monimuotoinen arkkitehtuuri tulee vaatimaan panostusta tietoturvaan. Jotta yhteiskunnan toiminta, käyttäjien yksityisyys ja luottamus palveluihin säilyvät, tulee tietoturvaan panostaa.

Perinteiset matkapuhelinverkot ovat melko staattisia, joissa jokainen komponentti on erikseen suunniteltu ja tietoturva-asetukset laitettu kohdalleen. Ohjelmisto ja laitteet tulevat yleensä samalta toimittajalta sisältäen selkeät suositukset tietoturva-asetuksista.

5G teknologiassa verkot eivät ole enää staattisia verkkoja. 5G-teknologiassa verkon tulee olla dynaaminen ja mukautua automaattisesti liikennetilanteen mukaan. Tietoturvan automatisointiin ja sen reaaliaikaiseen seurantaan tulee kiinnittää huomiota.

IT-järjestelmissä käytössä oleva virtualisointi tulee korvaamaan laiteratkaisuja matkapuhelinverkoissa. Matkapuhelinverkkojen verkkokomponentit eivät tule enää yhdeltä toimijalta, vaan laitteisto voi tulla yhdeltä toimijalta, virtualisointikerros toiselta ja virtualisointikerroksen päällä voi toimia useiden eri toimittajien teknologioita ja palveluita. 5G-teknologiassa myös verkko ja palvelut sitoutuvat kiinteämmin yhteen. Tämän seurauksena on todennäköistä, että palveluja tullaan toteuttamaan lähellä matkapuhelinverkkojen kriittisiä komponentteja. Perinteisesti matkapuhelinverkot ovat olleet operaattorien hallinnassa ja ulkopuoliset palvelut toteutettu verkon ulkopuolella internetissä. Matkapuhelinverkko ei ole enää operaattorin ylläpitämä muurein suojattu linnake. Kokonaistietoturvan merkitys kasvaa, koska arkkitehtuuri tulee olemaan huomattavasti nykyistä monimuotoisempi. Verkon ylläpitäjällä tulee olla ymmärrys ja vastuu kokonaisturvallisuudesta verkossa, jossa on useita toimijoita.

IT-järjestelmien virtualisoinnissa ja palvelujen tarjonnassa on selkeästi nähtävissä trendi, missä virtuaalialustoja tarjoavat monikansalliset toimijat, joiden palvelinkeskuksia on ympäri maailmaa. 5G-verkkojen tapauksessa on tärkeää tunnistaa ne toiminteet, jotka tulee pitää omassa hallinnassa itse ylläpidetyillä palvelinalustoilla.

5G tuo mukanaan heterogeeniset liityntäverkot. Nykyisissä verkoissa tukiasemat ovat olleet hyvin samankaltaisia ja operaattoreiden hallinnassa. 5G-teknologian myötä hyvinkin monimuotoisten tukiasemaratkaisujen käyttö mahdollistuu, mikä asettaa omat haasteensa verkon turvallisuuden hallinnalle.

2 Uudet palvelut tuovat mukanaan uudenlaisia riskejä

Traficom on tutkinut 5G-teknologian tietoturvallisuuteen kohdistuvia riskejä osana Traficomin omista tarpeista laadittua syksyllä 2019 käynnistynyttä 5G-tietoturvallisuusselvitystä. Myöhemmin selvityksen havaintoja käytettiin EU-komission pyytämän kansallisen 5G-riskiarvion muodostamiseen.

Keskeisimmät riskit 5G-teknologiassa aiheuttaa teknologisten ympäristöjen ja käytettävien arkkitehtuurien muuttuminen yhä monimutkaisimmeksi edellisiin matkapuhelinverkkoteknologoihin verrattuna. Tämä lisääntynyt monimutkaisuus teknologiassa ja palveluissa haastaa nykykäsityksen siitä, miten riskejä hallitaan ennakkoon ja miten toteutuneiden riskien syy-seuraussuhteet ymmärretään ja niiden vaikutukset rajataan digitalisoituvassa yhteiskunnassa. Alan nykyiset standardit ja määräykset eivät määrittele parhaita käytäntöjä tai toimintamalleja, miten arkkitehtuurit ja palvelut tulisi rakentaa turvallisiksi jättäen näihin liittyvät päätökset verkon toimijoille.

Lisäksi riskiä lisää uudentyyppisten palveluntuottajien mukaan tuleminen olennaiseksi osaksi 5G-ekosysteemeihin. Näitä uusia palveluita ovat esimerkiksi verkon reunalla ja lähellä käyttäjää tuotettavat niin sanottuun reunalaskentaan perustuvat hyötypalvelut jotka ovat olennainen osa esimerkiksi seuraavan sukupolven älyliikenteessä. Uudet palvelut pääsevät käyttämään verkon resursseja sekä keräämään käyttäjistä tietoja uudella tavalla, jolloin riskit käyttäjille ja verkon infrastruktuurille muuttuvat. Mikäli näitä resursseja halutaan väärinkäyttää tai niiden käyttö estyy esimerkiksi huonon ohjelmiston laadun tai haittaohjelmiston vuoksi voivat vaikutukset ulottua koko verkkoon ja yhden käyttäjän riskit levitä myös muihin verkon käyttäjiin. Yhden käyttäjän riski voi olla nyt myös muiden verkon käyttäjien riski.

Teknologioiden perustuessa yhä enemmän avoimiin standardeihin ja yleisesti saatavilla oleviin ohjelmistokomponentteihin, tulee myös 5G-verkkojen turvallisuuden hallinnan ja seurannan kehittyä kohti yleisissä IT-ympäristöissä käytettyjä menetelmiä. Samoja tietoturvallisuuden peruskyvykkyyksiä käytetään kaikkialla digitaalisessa yhteiskunnassa, eli 5G-teknologia ei edusta poikkeuksellista teknologiaa sen turvallisuudesta huolehtimisen osalta. On kuitenkin huomioitava, että matkapuhelinverkkojen yhteiskunnallisen kriittisen aseman johdosta, matkapuhelinverkot ovat säädellympiä kuin perinteiset IT-järjestelmät.

Edellisten sukupolvien verkkoarkkitehtuurissa voitiin määritellä missä kriittiset toiminteet pyörivät ja siten suojata ne. 5G-verkoissa palvelut todennäköisesti menevät lähemmäs käyttäjää sekä muuttua käyttäjien sijainnin tai sen hetkisen tarpeen mukaan. Tällöin myös verkon kannalta kriittisten toiminteiden sijainti voi muuttua. Etenkin liikenteen automaation sovelluksissa tämä voi tulla eteen. Muutoksesta johtuen kriittisten kohteiden tunnistaminen ja siten niiden suojaaminen tulee haastavammaksi.

5G-teknologian kehittyessä ja sen saadessa yhä tärkeämmän roolin digitaalisessa yhteiskunnassa, tulee uusia riskejä esiin myös tulevaisuudessa 5G-teknologiassa uusien ominaisuuksien sekä teknologiaan liittyvän tutkimuksen myötä. 5G-verkossa olevat loppukäyttäjien hyötypalvelut ovat kriittisyydessään ja tietosisällöltään houkutteleva sekä potentiaalinen kohde niin tavallisille hakkereille, kyberrikollisille kuin valtiollisille toimijoille.

3 Yrityksien tulee varautua riskeihin ja hallinnon tehtävä on ohjata ja tukea

Traficom tukee komission näkemystä siitä, että mikäli 5G lunastaa keskeiset lupauksensa, siitä ei tule vain viestinnän, mutta myös useiden yhteiskunnan muiden tärkeiden toimintojen, kuten liikenteen ja terveydenhuollon, kulmakivi. Tällöin systeemisten teknologisten heikkouksien vaikutus yhteiskuntaan olisi suuri. On siis varmistuttava myös siitä, että 5G-palveluita tarjoavien organisaatioiden riskinotto on linjassa yhteiskunnan riskinottohalukkuuden kanssa. Tätä on syytä tukea paitsi tuottamalla tietoa ja työkaluja 5G-palveluntarjoajien riskienhallintaa tukemaan, myös varmistamalla oikein kohdennettujen viranomaismääräyksien keinoin, että palvelutuotannon kyberturvallisuus on riittävällä tasolla.

Uudenkaltaisten toimijoiden tullessa osaksi 5G:n palveluntuotanto- ja arvoketjua, myös sääntelyn velvoittavuuden laajuudesta on syytä käydä keskustelua. Aiemmissa verkkosukupolvissa verkkoa on käytetty ensisijaisesti tiedonsiirtoputkena, mutta reunalaskennan yleistyessä verkossa vaikuttavat rinnakkain teleoperaattorin lisäksi monet muut toimijat.

Keinoina 5G:n myötä tärkeämmiksi muodostuvia, esimerkiksi komponenttivalmistajien tuotantoketjusta johtuvia riskejä vastaan, voidaan käyttää esimerkiksi verkkohankintojen hajauttamista useammalle toimittajalle. Tällöin on kuitenkin varmistuttava vianselvityksen prosesseista, verkon teknisen toimivuuden ja tietoturvallisuuden valvonnasta (esimerkiksi Havaro 2.0 avulla) ja lisäksi palveluiden yhteentoimivuudesta eri toimittajien laitteiden välillä. Palveluntuottajien ja teleoperaattoreiden tietoturvallisista menettelyistä varmistumisen lisäksi myös keinoja kansainvälisten laitevalmistajien tietoturvallisuusprosesseista varmistumiseen on harkittava, sekä kansainvälisenä yhteistyönä että kansallisella tasolla. Kansainvälisen yhteistyön tiivistäminen on tarpeen 5G:n kyberturvallisuusuhkien tunnistamisessa, 5G-järjestelmien turvallisuuden minimitason määrittelyssä ja järjestelmien vaatimuksenmukaisuudesta varmistumisessa. Suomella ei ole resursseja rakentaa näihin vaikuttavuudeltaan riittäviä ja tehokkaita sertifiointiprosesseja yksin. Hyvin yksityiskohtaisten teknisten sertifiointikehikoiden rakentamiseen Traficom suhtautuu varauksella 5G-verkkoympäristöjen jatkuvan päivitystarpeen vuoksi. Suomen on kuitenkin hyvä olla aktiivisesti mukana, jos Euroopassa aletaan kehittää sertifiointia. Tällöin pääsemme vaikuttamaan sisältöön ja olemme sisäpiirissä näitä kehittämässä, mikä on tärkeää myös Suomen teollisuuden kannalta.

Oman kulmansa riskeihin varautumiseen tuo mahdollinen megatoimijoiden, kuten Googlen, Facebookin ja Amazonin, tulo mobiiliverkkomarkkinaan. Jos 5G-verkko saa roolin käyttäjien sisältöjen käsittelyssä, siitä tulee houkutteleva alue näille toimijoille. Megatoimijoiden sääntelyn tarvetta määritettäessä tarvitaan tehokasta ja vaikuttavaa eurooppalaista yhteistyötä.

5G on Suomelle valtava mahdollisuus taloudellisesti ja kansalaisten hyvinvoinnin kannalta. Tätä tukevat 5G:n mahdollistamat asiat, kuten etäterveydenhuollon entistä parempi saavuttavuus. Kaikki suuret muutokset tuovat mukanaan riskejä, joihin varautuminen on päivittäistä toimintaa yhteiskunnassa. Varautuminen vaatii yhteistyötä, toimia ja päätöksiä, mutta 5G:n mukana ei tule mitään sellaista, mitä ei huolellisella riskeihin varautumisella kyettäisi hallitsemaan.